Technical Cybersecurity

Attacking Passwords

Brute Force

CAN'T GO BACKWARD

- We can't go backward from ciphertext to plaintext
- So we need to go forward and try various possible passwords until we find one that matches
- Cain, Hashcat, John do this
- Use dictionary files with mutation rules
- Effective, can be slow though
- GPU-based cloud computing for the win!

Rainbow Tables

Rainbow tables are precomputed hashes

- Basically just a table of possible passwords and associated hashes, where the hashes are generated via algorithms of interest
- Read the hash from the table, compare it to the hash you're trying to crack
- Can't use v. salted hashes (and unsalted hashes are rare today)
- With GPUs and modern computers, rainbow tables are less and less viable

Why bother cracking at all?

PASS-THE-HASH

- Take the hash and use it directly
- Metasploit can use a hash directly

HOW DOES THIS WORK?

- Passwords are not passed in clear text, they’re passed hashed
- The hashes are then compared on the target
- Without additional security around the hash (e.g. digital signature, or hash-of-hash with timestamp, or similar) you can just use the hash to authenticate!

Protection? Strong passwords and better algorithms.

Next up, malvertising, exploit kits, and phishing.